


MEMORANDUM

TO: State CIOs and State Security Liaisons

FROM: Maria S. Thompson 
State Chief Risk Officer

SUBJECT: 2018 Guidance for Annual Legislative Reporting of Security Assessment and Compliance – Continuous Monitoring

DATE: June 1, 2018

A. OVERVIEW:

The State Chief Information Officer (SCIO), is charged with ensuring State agencies and State data are operating in compliance with established enterprise security standards. To accomplish this task, the Enterprise Security and Risk management Office (ESRMO) has developed a Continuous Monitoring Plan (CMP) to address the management of risk assessments and compliance reporting throughout the state. The CMP is a program designed to monitor and ensure that all agencies are assessed using one or a combination of assessment methods identified below:

- Third Party Independent Assessment (Vendor or National Guard)
- Self-Assessment

The annual assessments and compliance reporting will allow Agency leadership to monitor cyber deficiencies and focus on assessing agencies progress toward achieving outcomes that strengthen Statewide cybersecurity while meeting legislative requirements.

B. GENERAL INSTRUCTIONS:

Pursuant to N.C.G.S. 143B-1376 the State CIO must annually assess the ability of each agency and each agency's contracted vendors to comply with the current enterprise-wide set of security standards. In addition, the State CIO is to annually certify by October 1, that State data held in non-State facilities is being maintained in accordance with State IT security standards. The information gathered from each assessment will be used to build out the State IT Plan. These assessments will include, at a minimum:

1. Rate of compliance with the enterprise-wide security standards
2. Estimate of cost to implement deficient security measures
3. Assessment of Security Organization
 - a) Security practices
 - b) Security industry standards
 - c) Network security architecture
 - d) Current expenditures of State funds for Information Technology (IT) security

This certification will be provided annually to the Joint Legislative Oversight Committee on IT and Fiscal Research Division. All agencies **MUST** complete an assessment annually. It is the agency's responsibility to ensure that an appropriate budget amount is requested to meet the needs of the legislative mandate.

Any deficiencies identified within the agency which would preclude them from being compliant, must be addressed using the Corrective Action Plan (CAP) template. Agencies are required to use the Corrective Action Plan spreadsheet located at <https://it.nc.gov/document/corrective-action-plan-cap-and-instructions>

C. ASSESSMENT GOALS AND TARGETS:

Security Assessments are required annually, as outlined in the CMP. The assessments are conducted on a 3-year cycle. **Agencies that have completed self-assessments in years 1 and 2 MUST complete a third-party assessment during Calendar year (CY) 2018.** The 3-year cycle begins again during calendar 2019.

ONLY those agencies that have completed a 3rd party assessment in the previous 2 years, have the option of completing a self-assessment during this compliance period. The self-assessment will be completed using the Department of Homeland Security, Cybersecurity Evaluation Tool (CSET). The framework that will be selected for use within CSET, is the NIST 800-53 revision 4 controls (Moderate). This framework provides agencies with a comprehensive structure for making more informed, risk-based decisions and managing cybersecurity risks across their agency. The CSET will facilitate the consolidation of agency reports and provide a summary of compliance with industry best practices and state requirements. Note: It is recommended that the assessment be completed using a cross functional team consisting of representatives from operational, maintenance, information technology, business, and security. The representatives must be subject matter experts with significant expertise in their respective areas.

To be considered compliant with a selected control, agency results **MUST** be $\geq 90\%$. The only exception for this year is cyber awareness training where the target goal for 2016 was 80%. Agencies which achieved 90% or better during 2017 are considered compliant.

The CSET application and self-assessment instructions are available for download from the ESRMO external SharePoint site listed below. Agencies are required to utilize the .cset file labeled "2018 Self Assessment_Moderate.cset". This file must be imported into CSET for completion. The file will contain pre-populated answers for those controls that are Enterprise controls. Agency liaisons must contact ESRMO if access is needed.

https://ncconnect.sharepoint.com/sites/it_ext/esrmo_ext/Documents/CSET/CSET%208

D. REPORTING DATE:

All state agencies are required to provide the State CIO with their annual compliance and assessments reports **no later than** September 1, 2018. This submission must include compliance of cloud service providers as well as corrective action plans to remediate any findings. Reports must be encrypted to protect the confidentiality of the information.

Agencies submitting self -assessment reports will include the following documents to satisfy this requirement:

1. CSET Assessment file (.cset or cseta (for merged assessments))
2. CSET Site Detail Report (.docx)
3. Appendix A – Compliance Report
4. Corrective Action Plan (if applicable)

Agencies completing a third-party assessment, need only provide the following:

1. Appendix A – Compliance Report
2. 3rd Party Assessment Report(s)
3. Corrective Action Plan (if Applicable)

The point of contact (POC) for this correspondence is the State Chief Risk Officer, Maria Thompson, maria.s.thompson@nc.gov, or (919) 754-6578.

APPENDIX A – AGENCY ANNUAL ASSESSMENT AND COMPLIANCE REPORT TEMPLATE

[AGENCY LETTER HEAD]

TO: Eric Boyette
State Chief Information Officer

FROM: [AGENCY]

SUBJECT: 2018 Agency Compliance Report

Pursuant to the authorities and powers of the State Chief Information Officer enumerated in Session Law 2015-241, and as Agency head for [AGENCY];

A. I certify that [AGENCY] has implemented the appropriate processes and procedures listed below to be in compliance with the Statewide Information Security Manual and State statutes:

- No data of a confidential nature, as defined in the General Statutes or federal law, was entered into or processed through any information technology system or network established under this Article until safeguards for the data's security satisfactory to the State CIO have been designed and installed and are fully operational.
- Agency obtained approval from the State CIO prior to contracting for the storage, maintenance, or use of State data by a private vendor.
- Agency ensured all information technology security goods, software, or services purchased using State funds, or for use by a State agency or in a State facility, was subject to approval by the State CIO in accordance with security standards
- Agency completed annual risk assessments to identify compliance, operational, and strategic risks to the enterprise network. These assessments may include methods such as penetration testing or similar assessment methodologies.
- Agency ensured all contracts for third party assessment and testing, was approved by the State CIO (as applicable), and resulting sanitized assessment reports were made public.
- Agency provided the full details of the State agency's information technology and operational requirements and of all the agency's information technology security incidents within 24 hours of confirmation
- Agency designated an agency liaison in the information technology area to coordinate with the State CIO.
- Agency completed an annual assessment of the agency's contracted vendors, to comply with the current security enterprise-wide set of standards. The assessment shall include, at a minimum, the rate of compliance with the enterprise-wide security standards and an assessment of security

organization, security practices, security information standards, network security architecture, and current expenditures of State funds for information technology security.

- Agency submitted disaster recovery plans to the State CIO on an annual basis and as otherwise requested by the State CIO
- Agency achieved completion rate ≥ 90 percent for annual Cybersecurity Awareness Training during CY 2017
- [AGENCY] has not completed all requirements but have identified a plan to be in compliance. Attached is our assessment report to include corrective action plan indicating when the agency will meet these requirements.

B. In accordance with § 143B-1342, below is the estimated cost to implement security measures needed for agencies to fully comply with the standards.

SECURITY / BUDGET DEFICIENCIES:

1. Security Boundary Devices:

[INSERT JUSTIFICATION/COMMENTS or N/A]

Cost to Remediate: _____

2. Personnel:

[INSERT JUSTIFICATION/COMMENTS or N/A]

Cost to Remediate: _____

3. Cybersecurity/IT Training:

[INSERT JUSTIFICATION/COMMENTS or N/A]

Cost to Remediate: _____

4. Vulnerability Management:

[INSERT JUSTIFICATION/COMMENTS or N/A]

Cost to Remediate: _____

5. End of Lifecycle Systems:

[INSERT JUSTIFICATION/COMMENTS or N/A]

Cost to Remediate: _____

For additional information about this submission please contact: [INSERT AGENCY CONTACT]

Printed Name of Secretary/CIO or Designee

[Date]

Signature of Secretary/CIO or Designee